AEROSPACE REPORT NO.
TOR-2015-02545

Design Review Improvement Recommendations

June 18, 2015

Richard K. Covington
Digital and Integrated Circuit Electronics Department
Electronics Engineering Subdivision

Prepared for:

National Reconnaissance Office
14675 Lee Road
Chantilly, VA 20151-1715

Contract No. FA8802-14-C-0001

Authorized by: Engineering and Technology Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement Workshop.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 JUN 2015	**Final**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Design Review Improvement Recommendations	**FA8802-14-C-0001**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Richard K. Covington	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
The Aerospace Corporation 2310 E. El Segundo Blvd. El Segundo, CA 90245-4609	**TOR-2015-02545**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
National Reconnaissance Office 14675 Lee Road Chantilly, VA 20151-1715	**NRO**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
2015 MAIW Product

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**38**	

Acknowledgements

This document was created by multiple authors throughout the government and the aerospace industry. For their contributions, we thank the following authors for making this collaborative effort possible.

Richard Covington, The Aerospace Corporation, co-lead
Steve Hogan, The Aerospace Corporation
David Pinkley, Ball
Kevin Paxton, Boeing
Frank Roller, Lockheed Martin, co-lead
James Fieber, Lockheed Martin
Mark Braun, Raytheon
Robert Lyon, SSL

A special thank you for co-leading this team and efforts to ensure completeness and quality of this document goes to Frank Roller, Lockheed Martin.

The authors deeply appreciate the contributions of the subject matter experts who reviewed the document:

Joseph Aguilar, The Aerospace Corporation
Roland Duphily, The Aerospace Corporation
William Tosney, The Aerospace Corporation
Barry Liu, Boeing
Mick Worcester, Boeing
Anne Ramsey, Harris Corporation
Ronald H. Mandel, Lockheed Martin
Mark King, Micropac Industries
Melanie Berg, NASA
Cindy Kohlmiller, Northrop Grumman
Derek Layne, Northrop Grumman
Jeff Cusick, Raytheon
Luis Garcia, Raytheon
Bill Hoehn, Raytheon
Ethan Nguyen, Raytheon
Dyane Peters, Raytheon
Donna Potter, SSL

Executive Summary

The aerospace industry continues to experience design escapes that significantly impact program execution and mission operations in spite of significant advances in design and analysis tool capabilities and robust command media governing the product development and design review process. This report presents the findings and recommendations from an MAIW industry team's evaluation of 170 design escape anomalies that were detected during either factory testing or on-orbit test and operations.

This analysis shows that a majority of these defects should have been detected and resolved earlier in the product development lifecycle. The primary factors contributing to these design review escapes have been shown to be:

- Failure to staff design review teams with individuals having the necessary domain expertise (60%)
- Failure to identify deficiencies in completed design analysis (30%)
- Failure to perform development testing using an Engineering Model (EM) to validate the design and supporting analysis (43%)

This report includes the team's recommendations for:

- Executing unit and lower level reviews including guidelines for selecting design review leads and ensuring the required subject matter experts (SMEs) effectively review the proposed designs at the appropriate time/review

- Establishing financial incentives that are tied, in part, to the successful completion of a fully integrated EM and its associated testing and verification prior to critical design review (CDR), independent of the CDR event

This report also includes recommendations provided by the industry team members to address additional issues identified in the supporting analysis, such as those associated with effectively reviewing integrated mixed technology products.

While these recommendations are targeted at Class A and B National Asset space programs, many of these recommendations can be implemented with little or no recurring costs and should be considered for all space programs to reduce the risk of a design escape going undetected and irreversibly impacting mission operations. Ultimately, the decision to implement these recommendations or not is based on the level of risk a program is willing to accept based on its design heritage.

The recommendations in this report complement, but do not duplicate, the recommendations provided in the following TORs:

- *Design Assurance Guide*, Aerospace Report No.TOR-2009 (8591)-11
- *Objective Re-use of Heritage Products*, Aerospace Report No. TOR-2013(3909)-1
- *Guidelines for Space Systems Critical Gated Events*, Aerospace Report No. TOR-2009(8583)-8545

This report does not address the Software Development Review Process given the uniqueness of the CMMI Process. The Software Development Process is extensively covered in TR-RS-2015-00012. The authors understand that the hardware/software interactions are an important part of any design development and that care needs to be taken to ensure the minimization of these adverse interactions. The team recommends that this topic be considered for a future MAIW topic.

Contents

Figures

Tables

1. Introduction

Mission Assurance Industry Workshop (MAIW) design review best practices were developed from a survey of national space program design escapes. This document provides the recommended design review tasks, along with the guidance on how to perform these tasks, and implement an effective design review strategy throughout a program's life cycle. Rationale and examples are provided as applicable.

This document is structured into two main sections:

- Section 3: Guidelines
- Sections 4 and 5: Lessons Learned; Case Studies

Section 3 provides a quick reference for best practice recommendations. Sections 4 and 5 are the details (the analysis) that lead to the recommendations.

2. Scope

As space systems become increasingly complex, the problem of identifying and correcting design defects becomes even more difficult. There are:

- new, state of the art electronic devices
- higher data rates
- increased levels of on-board data processing and storage
- higher imaging resolution
- higher sensitivities and increasingly complex real-time software giving rise to signal integrity issues
- EMI/EMC impacts
- hardware/software interactions
- complex mechanisms
- ever increasing impacts from the space weather environments

Recent design escapes identified during test and on-orbit demonstrate that the current design review process, while well documented and time proven in the past, has failed to identify issues as intended, only to have those escapes manifest themselves later in development flow or on-orbit. Refer to Section 5 for additional details on case studies reviewed for this document.

This document derives design review process improvements from escapes and corresponding case studies that highlight deficiencies or weaknesses in existing design review processes that allowed design escapes. For example, the application of new and emerging technologies with a low Technology Readiness Level (TRL) and the use of existing heritage in a different application or environment were identified as issues that push the limits of the existing design review process. The team analyzed best practices across industry and government agencies to prepare for and conduct design reviews.

Guidelines contained in this document are developed as they apply to Mission Class A and/or B, national asset vehicles with minimum practical- and low-risk profiles. It is understood that civil, commercial, and higher risk vehicle developments represented by Mission Class C and D, may bypass some of the checks and balances that are contained in this document, and should review the guidelines for merit to their specific Mission development risk. Provided in Appendix A are definitions for Mission Class A through D that bind their risk profile and thereby demarcate how these guidelines might apply.

For the purpose of this TOR, we have focused on the CDR, however many of the design findings are applicable to earlier design reviews, e.g., Preliminary Design Review (PDR), Internal Design Review (IDR), and any other detailed design reviews. This group has defined a design escape as a design defect detected after the finalization of the design which occurs at CDR.

The escape data (post CDR) gathered from surveys shows that the assembly development consists of ever increasingly complex hardware interactions with growing numbers of mixed hardware technologies within a single assembly. To adequately address these escapes the design review process requires the right skills to be applied at the appropriate level of the review to be effective.

2.1 Role of the Design Review

The role of the design review is to critically assess all aspects of the design through careful review of requirements compliance, verification, drawings, and analyses. The reviewers are the backbone of the design review process and are collectively responsible for the integrity of the design review.

Reviewers have the greatest impact at the technical level with access to design team and engineering products such as verification matrices, specifications drawings, test data, simulation, etc. It is important to get technical reviewers involved early and at this level of detail. This should not be confused with design review meetings or events that summarize findings and status of lower level reviews at a high level, which may be required by the customer. The survey data shows (Ref: Section 5, Table 5-3 Review Escape Deltas) that the PWB/PWA level escapes are not found until unit level or higher. These observations are review agnostic.

What is the role of the design reviewer? The most common role of the design reviewer is to verify that the requirements have been met and to prevent mistakes in the design, using their experience of past design errors, good engineering practice, and documented lessons learned to evaluate design aspects that do not meet requirements (performance, function, reliability, and quality), and to ensure that the program is managing their risks appropriately.

3. Guidelines

From the design escape data that was collected and analyzed, several high leverage items appeared. The rationale for each of the recommendations is in Section 5 case study analysis.

As part of the design review improvements charter, the government and industry team was asked to recommend codified changes and/or upgrades to the process that will effectively and efficiently identify and/or prevent design errors early in the program lifecycle.

While the product development and design review structure were found to be generally well defined, refer to Figure 3-1, the reviewer roles and responsibilities and the detailed review criteria were often less so. The design (assembly) *development* processes specifically in support of reviewers seemed to be robust, but the design *review* process was far less developed. The recommended changes are to the assembly development processes (instead of a separate reviewer process) so that the development team is aware up front what the reviewer needs, is expecting, and is expected to do. The team recommended that instead of creating a separate process for the reviewers, it is recommended that the development process be augmented with additional reviewer process content.

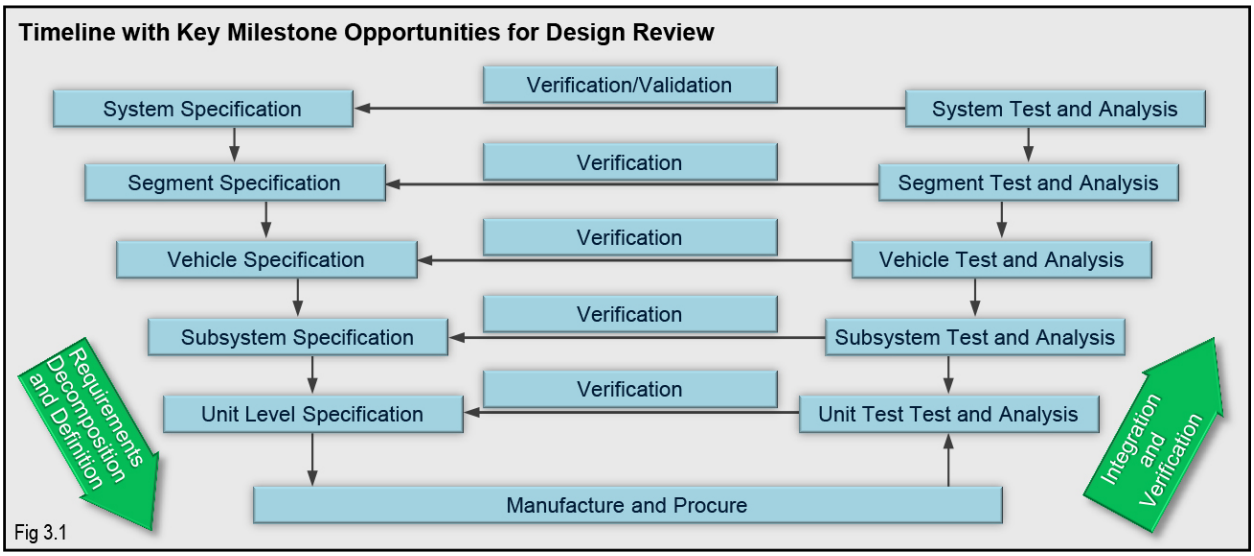

Figure 3-1. Notional development timeline with key milestone opportunities for design review.

3.1 Recommended Changes to the Assembly Development Process

The team developed key recommendations augmenting the design development process. The recommendations are intended as additions to the existing processes, but by themselves are not sufficient for a stand-alone reviewer process.

The team's recommendations are captured below with escape data and statistics followed by a specific recommendation in response to the survey findings.

In the case studies where 'inadequate design review' was the cause, 72% of the time the reviewers didn't have the proper skill set, refer to Figure 5-2.

- Ensure that the development process defines the minimum relevant domain experience to be lead or senior reviewer; they should be a recognized subject matter expert with the relevant material under review. Additional recommendations on reviewer selection are included in Section 3.1.2.

The case study data also showed that single reviewers for some efforts missed items that became design escapes due to relevant technical domain coverage. The types of developments below showed that one reviewer is not sufficient (requires multiple perspectives).

- Provide multiple cognizant reviewers for:
  - New PWB/Sub-ASSYs
  - PWB/Sub-Assemblies where
    - Prime/redundant on same board
    - High speed interfaces to another assembly
  - First time usage components (new technology and parts obsolescence applications)
  - Flight Software (FSW) reuse

During the survey of the existing development processes, it was found that there were robust processes and design standards for the individual technologies/disciplines (e.g., digital, analog, RF, firmware/software, power, mechanical) but what was found lacking was processes and standards addressing the unique requirements for mixed technology applications. The data also shows that design reviews conducted for mixed technology products frequently did not include subject matter experts with experience designing/reviewing mixed technology products. For example, a primarily digital sub-assembly had RF amplifiers in it. The reviewers for this sub-assembly had mostly digital and antenna RF experience, but were not RF PWB SMEs where isolation and cavity modes must be considered.

- Effort should be put toward developing technical standards and review criteria for products integrating mixed technologies

The case study data showed that many design escapes (33%) were associated with reused hardware where there was either a design change for obsolescence or change in application for a unit used without modification. This demonstrates the need to implement a rigorous review for hardware reuse against newly imposed requirements and appropriate regression test program.

- Guidance on the reviewing and validating reused hardware can be found in: *Objective Re-use of Heritage Products*, Aerospace Report No. TOR-2013(3909)-1;

Another significant finding from the case study data is that 90% of design review escapes that did not have a fully tested and verified EM prior to CDR could have been avoided had they had one.

- Ensure that there is a fully tested and verified EM before CDR
  - Data from EM testing is used to verify requirements
  - Reviewer can validate analysis results by direct comparison with test data
  - An integrated unit helps drive early discovery by highlighting potentially missing or inadequate requirements
  - Fully tested EM with other EM units (test bed) can be used in confidence tests at the sub-system or system level prior to system integration to reduce interface risks

- Ensure that the testing preformed on the EM captures
  - Four corner testing (including off-nominal cases as appropriate)
  - Test-Like-You-Fly (day in the life scenarios including endurance)
  - Data Throughput / Loading

- Power Cycling
- Environments / Dynamic conditions

- Incentive tied to EM testing complete in addition to CDR

The case study data revealed that inadequate analysis was present in 30% of the design escapes

- Ensure that the development process provides for the reviewer to review the analysis scope in context to the requirements as part of the design reviewer's tasks

- It is estimated that roughly 200-600 hours should be allocated for the reviewers. (This was determined by reviewing actual hours for the development and the total hours spent by the review team for a system-level review for a major space program. It is highly dependent on program heritage and review scope.)

- Ensure that the development process defines a minimum lead time, typically 30 days, for the reviewer to review the material

- The development team is required to provide the necessary material for the reviewer as early as 60 days and all the final products 30 days before the review
  - With the above in mind, it is better to have partial information early (with active engagement) than to review products late
  - Data is required earlier for designs with:
    - Mixed technologies
    - High Frequency Digital Design (> 0.5 GHz)
    - Complex power sequencing requirements
    - TRL $\leq$ 4

- Ensure that the development process defines a written set of reviewer expectations (from the lead's point of view). Refer to Section 3.1.4.

- It is recommended that the development team choose a set of independent reviewers early and maintain them as review resources for the duration of the program, updating as necessary as the development progresses.
  - Embedding experienced independent reviewers into the development process to provide real-time review and feedback to the design team reduces learning curve since the reviewers follow the process throughout development and may provide multi-program perspective

- Review of lessons learned as part of the development process, with a section in the review of the results of lessons learned review

- Robust lessons learned that are fed back into the design development process and command media

- Document in the discrepancies paperwork where, in the design review process, an escape occurred so that it can later be searchable and fed back into improving the review process

- For a given review, include a summary of the previous review findings and design solutions

- Reference *Mission Assurance Guide* Chapter 11; *Mission Assurance Reviews and Audits*, Aerospace Report No. TOR-2007(8546)-6018 Rev B; for ideas on analysis that need to be reviewed by appropriate SMEs at the various independent reviews

3.1.1 Entry and Exit Criteria Recommendations

3.1.1.1 General Review Criteria (SDR, PDR, etc.)

For general overview of entry and exit criteria review SMC Standard SMC-S-021 (2009); *Technical Reviews and Audits* for ideas

3.1.1.1.1 General Review Entry Criteria

Final Material available 30 days before review (early indicator of readiness)

Partial delivery of information encouraged early (prior to 30 days)

Senior reviewer assigned a minimum of 35 days before review

Lead reviewer must set expectations with the program and individual reviewer(s) and get commitment to meet those expectations

Reviewer time commitment unfamiliar with assembly / program: 10 hrs/wk for the 30 days implies 30 – 60 hrs minimum per subject matter area. Embedded reviewers or independent reviewers dedicated to the effort may not need as much time.

Reviewer(s) identified for each major discipline / technology

Requirements maturity is sufficient to allow review of the design e.g., for appropriate review level:

- Analysis completed, packaging solution identified and documented, etc.
- Test methodologies identified and complete

Reviewer and design team review the analysis plan and results for completeness

3.1.1.1.2 General Review Exit Criteria

All reviewer comments captured with closure plans

Senior reviewer stays on the review team until all action items have been closed. The review isn't closed until the senior reviewer says it is closed.

Actions require the issuing reviewer's concurrence for closure

Changes since previous review(s) need(s) to be captured and understood

Prior lessons learned have been researched, analyzed, and adapted as appropriate. A summary of relevant lessons learned should be made available for the review team.

Design changes reflected in the build documents and analysis/test data

All required drawings complete (for drawings not complete, need concurrence from review team, closure plans reviewed, accepted, and programmatic risks understood)

Required drawings represent the as-tested, as-built assemblies. Any differences between the flight design and that which was tested must be fully documented and understood.

Parts acquisition is on track

Risk mitigation plans identified and are on track

Design is consistent with planned CONOPS

Margins consistent with program standard for expendables and critical resources (power, memory, and throughput) exist

Margin budgets are met or mitigation actions are in place and tracked for insufficient margins

All analyses critical to CDR, the designs are complete

- For analyses not complete, an agreed-to closure plan with follow-up review

Assembly test complete and data is correlated to analyses and requirements consistent with the phase of the development

- For testing not complete, an agreed-to closure plan with potential impact identified including a follow-up review

Risk management is in place for any incomplete items

Lesson learned from the present activity have been captured and reviewed with the reviewers

3.1.1.2 CDR Criteria

3.1.1.2.1 CDR Entry Criteria

Final material available 30 days before review (early indicator of readiness)

A fully tested Configured Item EM verified per the specification requirements (TRL $\geq$ 5)

Partial delivery of information encouraged early (prior to 30 days)

Senior reviewer assigned a minimum of 60 days before review

Lead reviewer must set expectations with the program and individual reviewer(s) and get commitment to meet those expectations

Reviewer time commitment: 20 hrs/wk for the 30 days implies 60 – 120 hrs minimum per subject matter area. Embedded reviewers or independent reviewers dedicated to the effort may not need as much time.

Reviewer(s) identified for each major discipline / technology

Requirements defined (without any “To Be Determined [TBD]” or “To Be Reviewed [TBR]”)

- Analysis completed, packaging solution documented and complete, etc.

- Test methodologies complete, testing and verification of the EM is complete:
  - Four corner testing (including off-nominal cases)
  - Test-Like-You-Fly (day in the life scenarios)
  - Data Throughput / Loading
  - Power Cycling
  - Environments / Dynamic conditions

3.1.1.2.2 CDR Exit Criteria

All reviewer comments captured with closure plans

Senior reviewer stays on the review team until all action items have been closed. The review isn't closed until the senior reviewer says it is closed.

Actions require the issuing reviewer's concurrence for closure

Changes since PDR reviewed and understood

Prior lessons learned have been researched and adapted (suggest a discussion of this research with the reviewers)

Design changes reflected in the build documents and analysis/test data

All required drawings complete (for drawings not complete, need concurrence from review team, closure plans reviewed, accepted, and programmatic risks understood)

The production drawings represent the as-tested engineering model design. Any differences between the design and tested must be fully documented and understood

Engineering model and production to be discussed with the reviewers and if necessary, an EM retrofit / retest plan

Parts acquisition is on track

Risk mitigation plans identified and are on track

Design is consistent with planned CONOPs

Margins consistent with program standard for expendables and critical resources (power, memory, and throughput) exist

Margin budgets are met and mitigation actions are in place and tracked for insufficient margins

All analyses critical to proof of design are complete

- Performance to spec
- Engineering robustness
- For analyses not complete, an agreed-to closure plan with follow-up review

- Testing performed with BOL test requirement with EOL performance limit (as specified in the Configured Item specification)

Engineering model testing data is complete and correlated to analysis and requirements

- Performance
- Critical resources
- Accelerated Life testing
- EM to production equivalency review has been completed
- Appropriate interleaving of environmental and performance test has been completed
- Four corner testing (including off-nominal cases)
- Test-Like-You-Fly (day in the life scenarios)
- Data Throughput / Loading
- Power Cycling
- Environments / Dynamic conditions

For testing not complete, an agreed-to closure plan with potential impact identified including a follow-up review

Risk management is in place for any incomplete items and/or the production build

Up to date ICD, with external systems as well as between the development efforts interfaces are approved, **with no TBD/TBRs**

Lesson learned from the present activity have been captured and reviewed with the reviewers

3.1.2 Selection Criteria for Reviewers

The design defect survey data indicated that 72% of the design escapes were caused by having the incorrect skillset on the review panel (see Figures 5-1 and 5-2 for additional details). Given the significant number of issues identified with skillset failures, the MAIW Design Review topic team solicited each individual team member's company to review their processes and procedures for concrete examples of reviewer selection criteria. The general response was that industry documented the roles and responsibilities well, but specific qualifications outside of being a "subject matter expert" were less documented. The Design Review topic team identified four important aspects for assessing reviewer skillset:

1. relevant experience
2. review panel experience, from a programmatic point of view
3. independence from the unit under review
4. availability.

These four aspects and their importance are further expanded below with associated recommendations for process improvements.

Relevant Experience

Clearly, relevant reviewer experience is required for a review to be meaningful and successful. A credible reviewer, as documented by most industry processes, requires that reviewers have relevant experience or be SMEs. Unfortunately it can be difficult to quantify the relevancy of any given reviewer given its subjectivity. Experience is a life process driven internally and externally. Education-Aptitude-lessons

learned are just a few items feeding into this experience. Many times, lessons learned from other projects is how knowledge is transferred from one area to another, so having repeated exposure experience can be of great value. Education is another source. However, with technology rapidly changing, the person with the most relevant past experience may not actually have relevant current experience. Rather than focusing on knowledge certification processes, the working group thought it was more important to focus on how the review team was to be constituted. In the design escape database, many times the issue was not with a reviewer's lack of knowledge; the issue was that the specialty was not represented at all. It is not realistic to expect a really great digital designer to review an RF design, or perhaps something more subtle, a mixed digital/RF design alone.

The recommendation of the working group is for whoever is responsible for selecting the review panel, they should evaluate what kinds of technologies are involved and select reviewers familiar with those technologies. Those areas could include:

- digital design
- firmware
- software
- high speed routing
- RF
- mixed digital/RF
- thermal
- structural
- mechanical
- reliability (redundancy implementation)
- quality
- manufacturing
- etc.

Identifying what is new or difficult and matching the panel experience will provide far better outcomes. The integration of relevant design checklists can also significantly augment reviewer experience as well by forcing them to potentially think about the problem in a different way.

Review Panel Experience

Reviewers should have experience actually performing reviews. They should be familiar with the review process, what is expected of them, and what they should expect of the product team. It is difficult to set specific requirements to achieve these objectives, but the working group recommends the following be considered:

- Mentoring of a potential reviewer by senior reviewers either during a review cycle or multiple review cycles.

- Senior reviewer must be a recognized SME in the relevant technology. If not, then a more senior reviewer who has the appropriate skillset should participate.

The working group identified reviewer independence from both the assembly under review and the product chain of management as being critical to the success of a review. When design reviewers become overly familiar with a particular product complacency may creep in and jeopardize the ultimate quality of the review. A reviewer who is not fully independent may lose objectivity. They may overlook important details of the design, how it is used, and issues relating to recurring themes such as heritage re-use since

"it worked before." A fresh set of eyes is required to challenge all aspects of the design, identify potential issues and follow the trail of component requirements through to its final conclusion. In contrast a reviewer who is overly familiar with an assembly may have a tendency to jump to the middle or end of the design review process thereby risking escapes.

The other aspect of independence is programmatic. Most programs are challenged given short schedules and reduced budgets. Unfortunately this reality places increased burdens upon the reviewers to speed things up, a direct contrast to what they should be doing which is methodically concentrating on the details and asking the hard questions. Programmatic independence provides the structure which allows reviewers to push back and take the necessary time to do the job right and identify design defects without being concerned about programmatic repercussions.

Given the importance of independence, the working group recommends that the reviewers be either not working the program (best case), or not be working on another unit that has a direct interface to the unit under review or rely on its functionality/performance. While the working group feels that independence is important, it does not imply that all personnel on a review panel must be independent. Occasionally, lack of independence when associated with more in-depth knowledge or uncommon skillsets may still be advantageous.

Reviewer Availability

Reviewer availability is often a key aspect that is overlooked. Experienced, independent reviewers that have the subject matter expertise and provide constructive feedback are frequently in short supply. Unfortunately spending 1 hour on a 10 hour job adds very little value. As such, the working group recommends that a realistic assessment of the scope of the review be made up front and assure the reviewer can set aside that time when required. This time should include time to review design artifacts, participate in oral reviews as required, provide constructive feedback, and review/close review actions.

3.1.3 Required Technical Rigor

The technical rigor of a design review is directly proportional to the quality and amount of material available for review. A design is characterized by its engineering products abstracted to the level of the design review. Board level reviews must focus on the details that will make or break the design. Higher levels of reviews will tend to focus on how the units and subassemblies work together to provide functionality. It is important for higher levels of design reviews to assure that the lower level design reviews have taken place and to review any open issues identified at the lower levels. Lower level products (e.g., FPGA/ASIC, PWB/PWA) should be reviewed in the context of the integrated system (e.g., multiple subassemblies integrated to housing, multiple housings into an assembly). The design products for any review should include the following artifacts as applicable to the design review level:

- Functional/performance requirements and compliance
- Design/operational constraints
- Interface specifications and compliance
- Schematics and mechanical drawings
- Board artwork
- Part specifications
- Relevant firmware/software
- All relevant analyses results (performance, functional, operational, timing, producibility, etc.)
- All relevant test results
- Manufacturability and manufacturing plans

- Radiation requirements and compliance
- Maintainability to include design minimizing rework hazards
- Structural requirements and compliance
- Design Assurance (Reliability, PM&P, Radiation Effects, Testability, producibility, maintainability, …)

The design reviewer should work with the panel lead and the design team to identify the relevant material. Preliminary versions delivered early are preferable to final versions delivered at the time of the oral review.

The design defect survey indicated that 76% of the design defects should have been caught at the assembly (box/unit) or lower level design reviews.

This indicates that the highest return on investment is to focus on the sub-assembly and lower level review. Additionally, many of the design defects at the assembly level are found during initial test, thus indicating the value of test data. Unfortunately, very small defects at the ASIC/PWB/Unit level can be very challenging to detect by review alone. Engineering design tools and use of engineering best practices have made the design process more robust, but lack of knowledge about a specific process or part can cause design defects. This Design Review topic team highly recommends that equipment testing and supporting drawings be done to support reviews as soon as possible. The topic team also highly recommends engineering model test data at the relevant level be available by CDR (last design review prior to production build) in order to mitigate these issues.

3.1.4 Review Team Leader/Member Responsibilities

There are two critical roles in the design review process: the review team leader and review team members. The working group recommends the following responsibilities for each role to assure a smooth design review process.

Review Team Leader

- Coordinate the scope/schedule/cost/status of the review with program management
  - Review leader responsibilities do not end with the CDR presentation, they extend to ensure that the Action Items are addressed and closed with the appropriate reviewer.
- Identify critical aspects of the design to scope team selection
- Identify candidate team members and coordinate approval with program management
- Coordinate review schedules with team members
- Review entrance criteria and supporting documentation. If inadequate, notify program management of "do not proceed" conclusion with a minimum of 10 days in advance of the review.
- Set expectations of review team. Conduct training as required
- Coordinate the identification/distribution of review materials
- Coordinate and chair any oral presentations as part of the review
- Make recommendations on whether ready to proceed or not based on the review findings

- Coordinate briefing/report on design shortcomings and recommended solutions
  - Bring specific examples of deficiencies with associated risks in order for the program to discuss with the reviewer. Examples are: Analyses that do not close, e.g., unmitigated technical risk (e.g., negative margins); key requirements that are not implemented in the design; Key EM test data not available;
  - Work with lead to develop cost/schedule impacts)
- Ensure all findings are closed out by an independent entity

Review Team Member

- Understand expectations of the review team and associated responsibilities
- Set aside required time to complete review
- Identify expected review products. Coordinate with design team on availability
- Review design artifacts prior to any oral presentation
- Attend and participate in any oral presentation
- Identify design issues or potential issues
- Make recommendations on corrective actions. Coordinate impacts with design team
- Review corrective action material and continue to make recommendations
- Track corrective actions to closure

3.1.5 What and how data needs to be included in the failure report

The review of the current EM test data and past failure modes is crucial to making the right design trade-offs that will provide the best over-all value. Reporting and reviewing these past failure modes is necessary to creating a closed loop system. The team agreed that as part of this data analysis, there should be a risk assessment. Each risk should have a mitigation plan with a trigger for when management needs to get involved.

To provide an upfront awareness, relevant failure data / information should be available prior to the start of the design. This information will provide both the designers and the reviewers the knowledge and risk assessment to prevent future design escapes.

Based on findings from this Design Review Study, it is recommended that the following data or information should be included as part of the proactive design review process:

- High risks from the updated Failure Mode Effect Analysis (FMEA) and Fault Tree Analysis (FTA)
- Results from the review of lessons learned
- Understanding of the environmental requirements with margins (i.e., temperature, vibration, radiation, aging, etc.);
  - Take a profile of actual environmental conditions and document in application notes
- Review of relevant past GIDEP and field recalls
- Part obsolescence changes forecasted
- Mechanical deflection analysis based on vibration and vacuum environments
- Results from Critical Dimension/ICD review and mechanical tolerance stack up
- Adequately analyze inter-unit end-to-end interfaces between prime and subcontractors

- Analytical methods used for predicted margins

During the design review the above data / information is presented with a report-out on relevant past failure risks. This failure report-out should include the following:

- How these past risks are prevented / mitigated
- Barriers that are preventing the design optimization
- New likelihood of occurrence and impacts based on design improvements
- Recommendations to move high risks to the program's risk register

All failure data should be documented, tracked, analyzed, and updated in a closed-loop system for current and future reuse. Lessons learned databases, FRACAS (Failure Reporting, Analysis, Corrective Action System) and FMEA library are some methods to store this information. As discrepancies occur the data should be captured and made available to the design team and design review team. These storage locations will provide an opportunity to group similar issues, perform trend analysis, and prioritize issues to effectively utilize resources. By having these issues in common databases, they can be reused for future projects and production support.

A robust FRACAS is a key element in providing a failure report. To be useful the FRACAS should have the capability to easily sort by key fields, systems, subsystems, and failure modes. Appendix B contains an example of seven key steps that should be included in a FRACAS to support a failure report.

4. Lessons Learned

4.1 Current Design Review Practices

Independent technical reviews are held in advance of major program milestone reviews, including:

- System Requirements Review (SRR)
- System Design Review (SDR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Critical Integration Review (CIR)

The current design review practices and recommendations for improvement are summarized below.

These independent reviews are held as many as 90 days prior to the actual milestone review, to allow the program time to incorporate as many change requests as possible. The review team consists of a chair and has members representing each technical discipline that's relevant to the program of interest. Team members use a checklist to guide their reviews, and the items on the checklist are based on lessons learned from previous reviews. Checklist items cover the major technical support functions across all program phases, and even include entrance and exit criteria for the independent review.

Programs have the right to approve the members of the independent review team, and are also allowed to tailor the checklist for items that don't apply. Programs have to provide justification for excluded checklist items, however. The independent review team chair also is allowed to push back on excluded items, if appropriate. Programs plan for these independent reviews by providing budget, adding additional time in their schedule, and making their personnel available to answer questions and respond to action items.

The actual review begins with a program in-brief, where program personnel brief the independent team on the program, its driving requirements and design approach, and its most critical risks. The team then spends several weeks reviewing and evaluating program work products, and may consult with program personnel during that time.

The review team members use the checklist both as guidance and as an evaluation scorecard. Each checklist item is color-rated by a reviewer, with the color indicating the level of perceived risk. For example, reviewers may find some analyses or design documents are immature or unavailable, and will assess the risk of the program moving forward with those analyses or documents in their current condition. It's important not to lose sight of the products and the review of these products in order to come up with an appropriate assessment.

Once the review is complete, the review chair compiles the inputs, findings, recommendations, and action items into a single, overall report. This report is then briefed to program executives, along with the Chief Engineer and the Senior Mission Assurance representative assigned to the program. Any additional actions that result from this briefing are passed along to the program POC (usually the program manager) for closure. Action items and recommendations made by the review team are actively tracked to closure by the review board chair and the program POC. The reviewer that generated the action also needs to be part of the closure to ensure that the issue that was brought up is being addressed. Open actions from completed reviews are addressed at the engineering director level to ensure acceptable closure plans are in place.

4.2 Lessons Learned

Lessons learned described in this section are either missing or inconsistently incorporated into industry design review processes.

Systems level reviews don't always provide the level of detail required to prevent design escapes. The data collected and evaluated for this study concludes that the lower level reviews are where the leverage is, as opposed to the major milestone reviews, like CDR. Also key to preventing design escapes is the conveyance of clear unambiguous requirements without TBRs or TBDs prior to CDR. Experience in analyzing design escapes also point to the fact that it's not just new hardware that needs additional scrutiny, but modified hardware or previously flight qualified hardware used in a new application or a new environment. In the case of hardware reuse, it is extremely important to understand the context of how the hardware was originally qualified and how it will be used in the future. Qualification creep is a common derailer to a successful reuse application since the changes can be subtle. Fully understand and assess the requirements against the conditions in which the equipment was qualified in order to verify that it is enveloped.

Our data doesn't conclude that more design reviews or more participants in a given review reduce the number of design escapes. This simply puts a greater burden on programs for little added benefit. Programs should ensure that the expertise of the review team covers the relevant technical domains used in the design. Instead, programs should consider expanding the scope of existing reviews to include more robust lower level design reviews. Programs and independent reviews are always trying to strike a balance between time spent on the review and the quality of the review – more time spent on a review doesn't necessarily mean a better review. It does mean that the right reviewers at the right review will greatly reduce the chances of an escape. In addition, reviews work best when the program considers it an opportunity to get valuable feedback from SMEs, rather than a burden to be endured.

Reviews should focus on the quality and robustness of the design, and not necessarily on design process compliance or maturity standards (i.e., not grading the checklist, yet reviewing the design for any potential deficiencies). Independent reviews are generally conducted at the system level, and are often aimed at ensuring compliance with product maturity standards and other work processes or instructions. As such, they are not intended to be low-level design reviews, but more of a work product maturity and design process compliance assessment. It is recommended that these independent reviews extend down into the lower level reviews, as the study data shows that independent reviews at these lower levels will have a greater chance of discovering potential deficiencies.

Review of a design may require more than one reviewer. In addition, the reviewers should include technical experts from the different areas and technologies that the unit consists of (e.g., for a unit that contains an RF front end, digital processing and a secondary power converter; then the reviewers should consist of Digital, Power, and RF experts).

Technology development efforts should have a fully tested and verified Engineering Model (EM) available before CDR. This allows a design review team to more fully evaluate the design and its performance as well as provide a solid foundation for moving to flight design. This means that if the unit is primary/redundant, then the EM should also be primary/redundant, with both sides fully tested and verified.

Reviews should start early enough to allow lower level designs to be evaluated. The significant lead time (as much as 60 days) means that in some cases the review team is working with immature or incomplete design information. As a result, independent reviewers need to be flexible and patient in case of late-developing program products.

Better consideration needs to be given to the selection of independent reviewers. The most senior designers are not always the best qualified, as they may not have relevant experience with newer technologies, for example. Bottom line is to get the right reviewer at the appropriate review at the right time in order to best utilize their experience and knowledge.

Maintain continuity of the review team. The independent review team is composed of the same members for each of a given program's reviews, to the extent possible. This makes each review more cost and time effective, and results in a more comprehensive review.

A design review checklist should be based on lessons learned from previous reviews. A checklist should be a living document that evolves over time as technologies and processes change. The checklist should be a standard, configuration-controlled list, so it's uniformly applied (before tailoring) to all programs consistently. There can also be several versions of the checklist, each one tailored to the expected maturity of the given design review (PDR, CDR, CIR, etc.) in question.

Tracking action items to closure, using whatever resources necessary, communicate the importance and impact of the review to the program, the customer, and the review team.

4.3 Program Benefits

The current best practices for independent reviews described in Section 4.1 incorporate the lessons learned discussed in Section 4.2. As a result, programs benefit by being subject to a review process that has been streamlined, and focused on historically high-risk design review elements. These design review best practices provide greater confidence of capturing design issues up front, in-line with the design effort, thereby avoiding late escape I&T problems or potentially on-orbit escapes and their cost and mission impact respectively. Test beds also provide the opportunity to analyze interfaces and other interconnected elements.

More importantly, for the cost of a few hundred hours of labor (typically), programs have a much greater chance of avoiding design escapes that have cost tens of millions of dollars, and sometimes much more, to address.

Programs benefit from these independent reviews in several other ways as well. The primary benefit is that it results in better and more mature program work products, including designs, analyses, plans, and drawings. Because the reviews cover all program phases, other non-design related elements like schedule, facilities, staffing, funding, tooling, and equipment are also evaluated for expected maturity and risk. An additional benefit is that programs are able to provide evidence to their customers they've undergone and passed a comprehensive independent program review, which gives the customer greater confidence in the system under development. Additionally operational benefits of an EM extend to subsystem / compatibility testing, software development, and anomaly resolution.

5. Case Studies

5.1 Summary of Current Design Review Practices

The data investigation for the design review improvements effort investigated the causes of design escapes (an error or test failure discovered after assembly CDR). The team was tasked to determine:

1. Identify strengths and weaknesses of the current design review process at the component/unit/box level and below

2. Recommend codified changes and/or upgrades to the process that will effectively and efficiently identify and/or prevent design errors early in the program lifecycle

3. Recommend updates to the entrance and exit criteria for the design review process

4. Recommend criteria for the selection of independent design reviewers with the proper subject matter expertise

5. Define the level of technical rigor required to successfully prepare for and conduct a thorough design review

6. Define the actions to be taken when deemed not ready to proceed with the design review

7. Identify programmatic benefits for conducting a thorough technical design review

In pursuit of understanding the current practices, the team surveyed the participating contractors on details of their respective design review processes. Questions were asked to determine the maturity level of the process the reviewers follow (in contrast to the development process). Eight questions were asked of the contractors, with two responses.

- Reviewer minimum experience if any?
- Minimum time for reviewer to have the material in advance of formal review?
- What requirement, if any, for relevant reviewer experience?
- How mixed technology assemblies are handled (digital, RF, Analog/power, and FSW) from a Design Review perspective?
- How action items are documented and how is follow through formalized for closure?
- How are reviewers selected?
- What are the reviewer responsibilities?
- Is there a documented reviewer process?

The survey results identified that there was no consistent process for the design reviewer (as opposed to the development process). The detailed findings are:

- There is a development process, but not a “reviewer” process
  - One process requires the reviewer to “grade” the review, i.e., to generate “metrics”
- No reviewer minimum experience required
- No minimum time for reviewer to have the material
- No requirement for relevant experience

- The assembly review assumes the artwork has been reviewed at a lower level, thus not reviewed at this level
- No effective process for mixed technology units (digital, RF, Analog/power, mechanical, and FSW are all separate processes, reviewed separately)
- Action item follow through and closure needs better adherence (in some cases, action item metrics are driving the acceptance/rejection/reclassification of action items)
- One process required getting comments back to the lead three days before the review meeting)
- Signal integrity is showing up as standard, yet not in all command media

This data suggests that a more formal reviewer process is needed. It does not need to be its own process, but an enhancement to the development processes appears to be in order.

Since there appears to be no process for the design reviewer (instructions) to implement, other than follow the development process, the team examined 170 design escapes in two groups to determine if there was a pattern to the escapes and if there is a need to create a design review process, (or improvements to the development process). Group 1 data is a set of failures related to design escapes provided by the team members (49), extracted from a set of questions. Group 2 is a set of on-orbit anomalies compiled by The Aerospace Corporation over 12 programs (the data is classified). This group consists of 121 anomalies, with (79) being design related.

5.2 Group 1 Data

The team members were asked to answer the survey in Table 5-1:

Table 5-1. Survey Questions

1	Issue Description
2	How found?
3	When found?
4	If not found on first unit, where was first unit?
5	Primary Impact
6	Briefly quantify impact
7	Was the established development process followed?
8	Root Cause of Escape
9	Briefly summarize root cause of escape. Where should it have been caught earlier?
10	Should this have been caught in Design Review?
11	Should this have been found at a lower level?
12	Where should have this escape have been found? (At what level?)
13	Summarize: How could design review process have caught this mistake?
14	(More thorough? better independent experts?)
15	Tested EM unit at CDR?
16	Any additional commentary useful in understanding this issue
17	Lessons learned
18	What was the reviewer escape (Skill, time, process, resources?)
19	Would a fully tested EM to support CDR caught the escape?

The results of the survey were simplified (to turn many verbose answers into short, sortable answers) and filtered. The design escape cause results are shown in Figure 5-1.

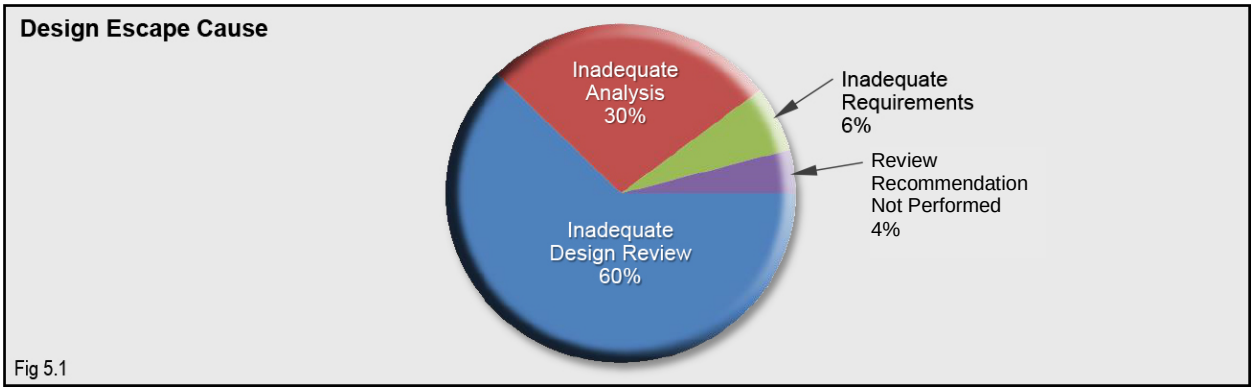

Figure 5-1. Design escape cause.

Survey results identified that ninety percent of the time, design review or analyses miss the defect. Note that Worst Case Analyses misses are included here as the review is supposed to catch any incorrect design analysis). Of the inadequate design review causes, the findings are that seventy-two percent of the time, the reviewer did not have the right skillset for the review (not getting help, not the right person). Figure 5-2 shows the breakdown of the causes behind the design review escape.

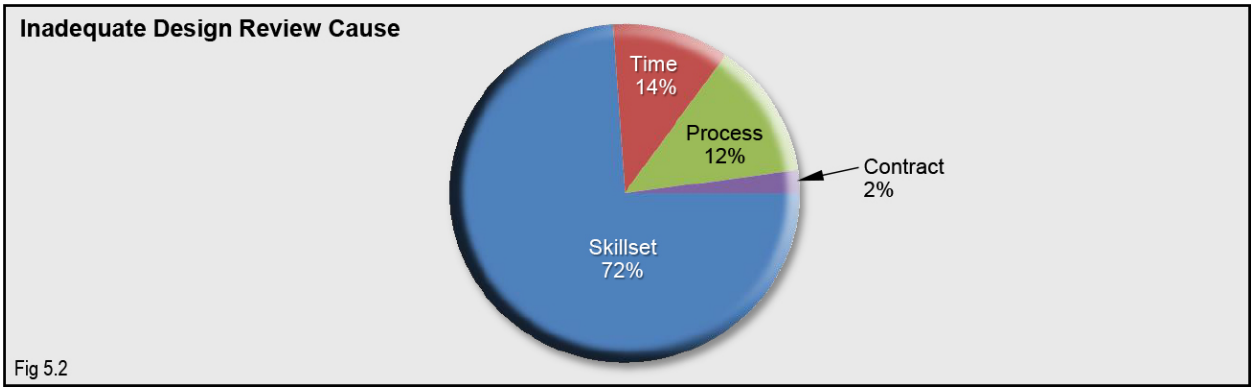

Figure 5-2. Inadequate design review cause.

Other observations in the data:

The authors consider process and skillset escapes are really process escapes.

It is interesting to see in what development phase the design escapes were found, (note, by definition, a design escape is after CDR), and where they could have been found. Post-CDR entries are late finds in the unit testing or design changes not fully tested i.e., the EM is not fully tested by CDR (Environments, integrated with FSW). Figure 5-3 shows where the escapes were found.

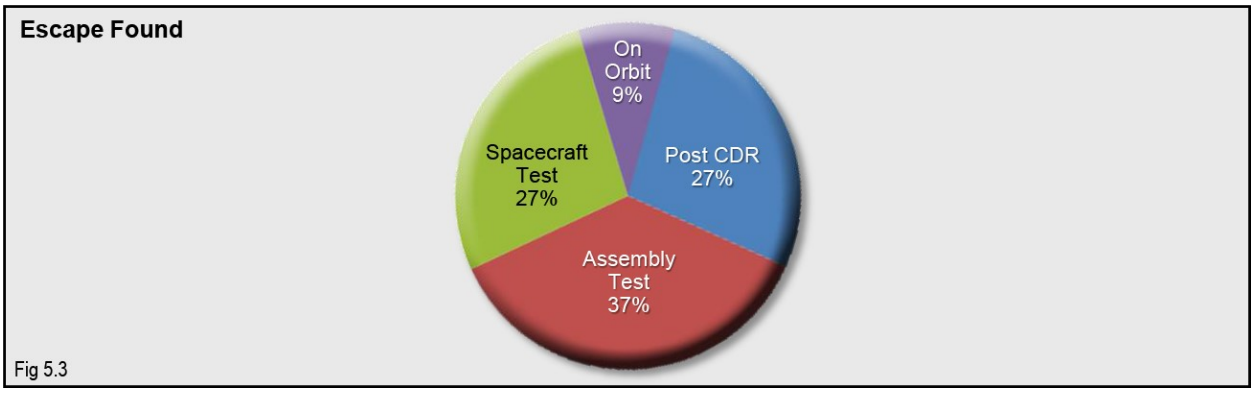

Figure 5-3. Escape found.

A scale was developed to find out the difference between where the escape should have been caught vs where it was caught. The scale is shown in table 5-2. The intent of the scale is to allow some degree of quantitative assessment of the escapes. Each escape was assessed by the team to determine where the escape should have been caught in the review process. Figure 5-4 shows the results of the assessment.

Table 5-2. Review Scale

Level	Gates
ASIC/FPGA/component	1
PWB/ASIC/FPGA review	2
Sub-Assy Dwgs	3
Sub-ASSY/FSW review	4
ASSY test/dwgs	5
ASSY review (CDR)	6
First ASSY test	7
Spacecraft test	8
On orbit	9

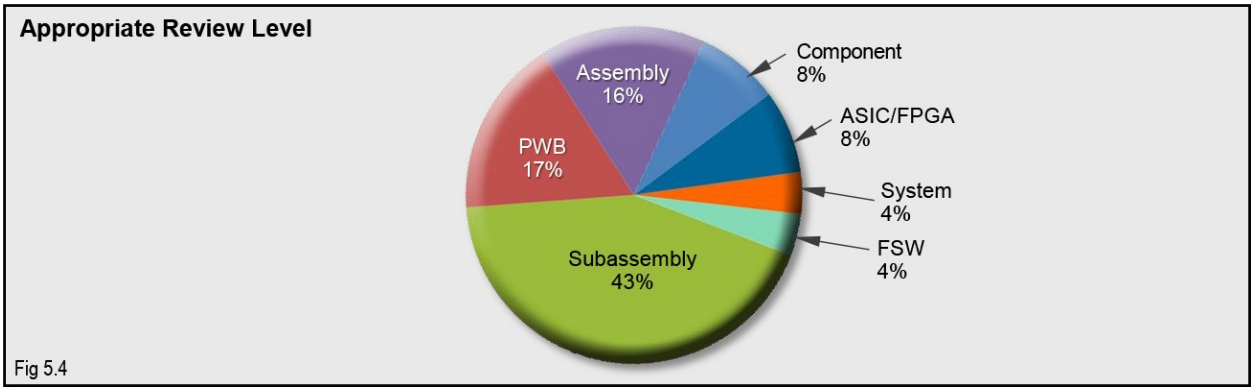

Figure 5-4. Review level where the escape should have been found.

Note that the level at which these escapes should have been found is relatively low.

It also turns out that the impact of these types of defects is high, with an average delta of 4 (between where a review should have caught the escape and the actual find), using the scale above in Table 5-2.

Also notice that many of the escapes are lower level escapes (PWB, Sub-Assembly, FSW (lumped into sub-assembly for level of detail).

So, is the testing at sub-assembly or assembly level lacking? Is the review at these low level, detailed areas lacking?

The data for escapes found at spacecraft test are that the test environment isn't high enough fidelity to bring out the defect.

Using the above scale, the average escape got by two reviews. When a deeper look is taken at each of the review escape types (PWB, Sub-ASSY, FPGA/ASIC) some trends show up and are shown in Table 5-3 below.

Table 5-3. Review Escape Deltas

avg PWB delta	5.5	three reviews
avg sub-ASSY delta	3.1	two reviews
avg ASIC/FPGA/Component delta	4.6	two reviews

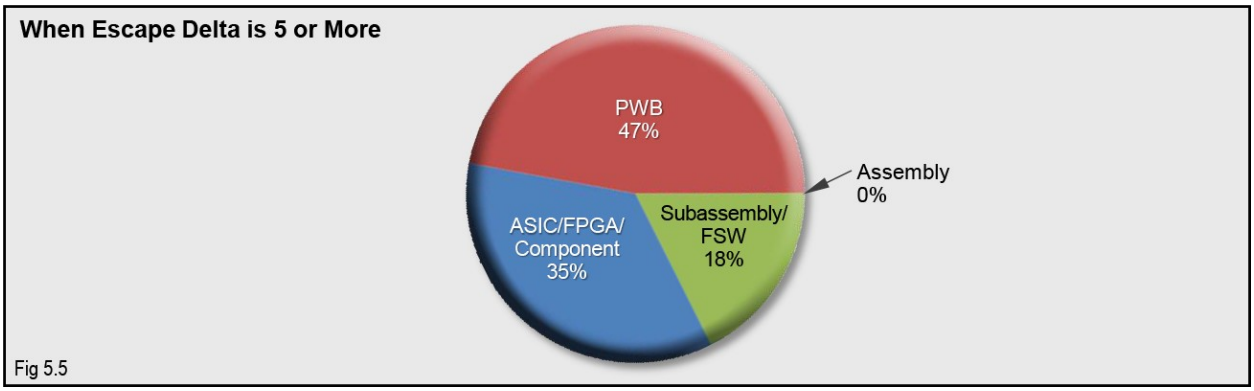

Figure 5-5. Areas where escapes are missed.

The high leverage reviews, those with a delta of 5 or more (indicating three review cycles have occurred before the escape was detected) are shown in Figure 5-5. These are the PWB/Sub-assy level reviews. The ASIC/FPGA/Component reviews are also high leverage, but tend to get caught at assembly test, (a bit artificial due to the definition of the design escape time frame). Component issues show up mostly due to changing a component for obsolescence reasons, (poor delta design reviews, poor EM regression testing), testing is recommended to include the entire test suite that the original design went through.

Other Interesting Data:

For the escapes that did not have fully tested engineering models, all but two (of twenty-one) would have caught the escape (all of these escapes were caught in testing), shown in Figure 5-6. This data led to the recommendation that fully tested engineering models (EM) be used to support CDR. Since CDR is typically an incentive milestone, this teams recommends that some portion of the historical incentive be tied to the completion, (and correlation of the EM data to analysis and requirements), of the EM test, not solely to CDR.

A technical escape topic that surfaced many times during the data review was unit to unit interfaces. Eleven of the forty-nine cases showed this as an issue. In addition, thirteen of the forty-nine cases involved the scope of the analysis/review (too narrow of focus), and ten of the cases involved the application of a component or assembly for a task it was not intended for. For the application related escapes, the reviews were along the lines of a partial review, not a full review back to the requirements and analysis (just updates). The examination of this data led to the recommendation that there should be multiple reviewers for new high speed interfaces; that design changes due to obsolescence and changes in application, (component, assembly), also need a rigorous review and retesting; and that reviewers need to add review of analysis scope as part of the design reviewer's tasks.

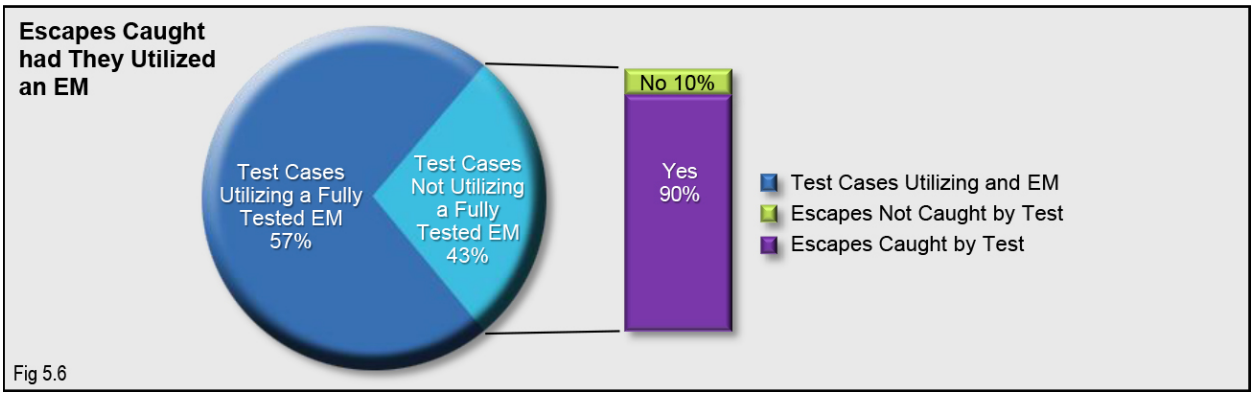

Figure 5-6. EM testing to catch escapes.

Hardware-Software interaction concerns and issues are well known. The data cases collected include only two cases of the forty-nine test cases and three cases of the one hundred twenty-one cases, which is insufficient to draw any meaningful conclusions.

5.3 Group 2 Data

The group 2 data was derived from a database of on-orbit anomalies. The group 2 data shows rough correlation to the group 1 data. The group 2 data does not have the same level of fidelity as the group 1 data, so only rough correlations can be made. Figure 5-7 identifies the approximate cause and Figure 5-8 identifies the level at which the defect should have been identified. The group 2 data does reveal that the average delta was 5.3 (not a surprise given that the dataset is comprised of on-orbit anomalies), resulting in an average of three reviews between where the escape should have been caught versus where it was caught, placing PWB reviews as the highest leverage review to have qualified, engaged, and aggressive reviewers (multiple).

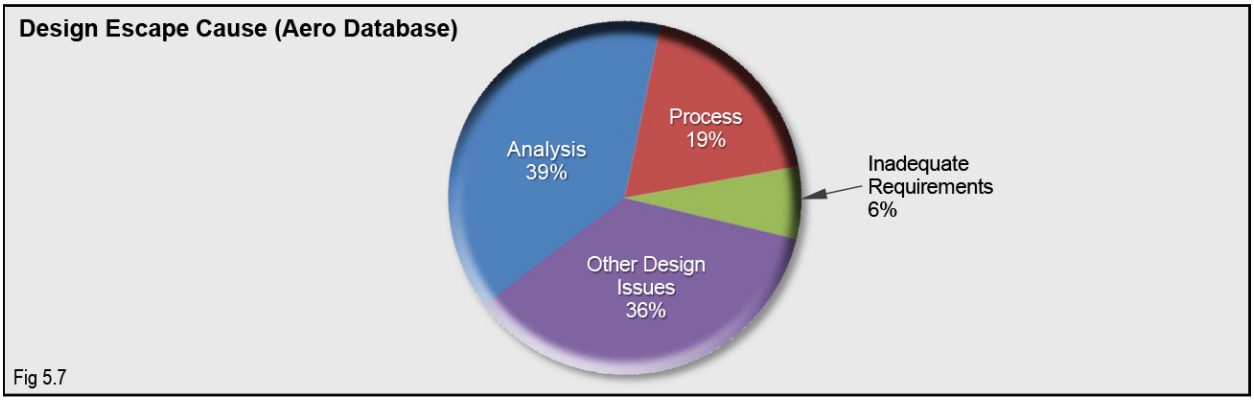

Figure 5-7. Design escape cause (Aero Data).

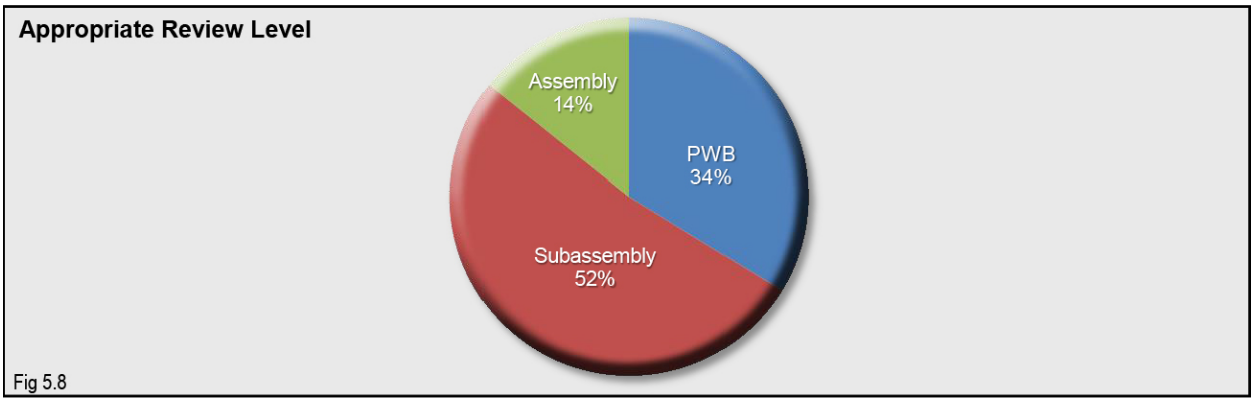

Figure 5-8. Review level escape should have been caught (Aero Data).

Appendix A

A.1 Definitions of Terms

Anomaly: Any deviation from expected performance associated with remotely operated elements(s). Anomalies (and faults) can include hardware failures, recoverable hardware upsets, infrequent extreme environmental conditions, or operator errors.

Assembly: A collection of sub-assemblies to form a configured item for installation onto the space vehicle.

Beginning Of Life (BOL): The start of the assembly's life cycle, pre-radiation and life effects.

Critical Design Review (CDR): A multi-disciplined technical review to validate that the design is complete and ready to proceed to production. A CDR is defined in this document as a series of design reviews that culminates in a higher level summary presentation.

Design Cycle**:** The period of time where the requirements are applied to create a product. The design cycle starts with the creation of requirements and ends with the start of manufacturing of the product or code delivery (CDR). A generic design development timeline is shown in Figure 3.1.

Design Development Process: A technical review of an assemblies design aspect for compliance to requirements and good engineering practice.

Design Escape**:** A non-compliant requirement, missing function, or out of tolerance condition found after the completion of the design cycle. Note: Any design defect on any test article discovered after CDR. For example, a design issue found on or from a First Article after CDR.

Design Review**:** The detailed critique of a design (documentation, drawings, analysis, and test data) by independent reviewers relative to formal requirements. The detailed review should not be confused with a summary presentation of lower level reviews (e.g., Critical Design Review Event).

Design Review Process: The complete set of actions in preparation for product release that includes the material preparation, reviewer selection, the design review, design review meetings, action items and responses, build control, and design review close-out.

Design Reviewer Process: The methodical steps the reviewer is responsible to perform when reviewing an assembly.

Independent Review Team: A team encompassing the Mission Assurance Team (MAT).

Independent Reviewer**:** A reviewer with relevant experience, external to the program or an internal reviewer that if working the program, does not have an interface to the item under review from their own effort (payload vs spacecraft, for example).

Preliminary Design Review (PDR): A multi-disciplinary technical review to assess the preliminary design of a product, establishing the product's baseline design.

Printed Wiring Board (PWB): The circuit board used to mount components and create circuits.

Space Vehicle: A craft capable of traveling in outer space; technically, a man-made craft in orbit around the earth.

Space Vehicle Anomaly: Unplanned event or series of events potentially resulting in damage or loss of mission.

Specialized Test Equipment (STE): Non-flight equipment used to test equipment intended for flight use.

Sub-Assembly: The collection of the printed wiring board, the mounted components, connectors, and mechanical structure to form part of the assembly. A sub-assembly may also be just the mechanical, electrical, electromechanical, electro optical, mechanical structure and/or mechanism, etc.

System Design Review (SDR)

System Requirements Review (SRR)

Verification**:** Methods used to show specifications are met.

Printed Wiring Board (PWB): The circuit board used to mount components and create circuits.

A.2 Class Definitions

Class A

National asset space vehicles generally support the national security of the United States. Class A space vehicles are the lowest risk (all practical measures are taken to reduce risk), highest importance to national security, highest confidence of success space vehicle (the highest procurement and assurance standards are used) with required long on-orbit life for a given orbit. Class A is reserved for space vehicles for which mission failure results in

1. an unacceptable collection gap, an unacceptable delay of a new capability, or an unacceptable reduction of capabilities,

2. a potential human safety hazard, or

3. a security breach.

A Class A space vehicle is an operational asset.

Class B

A national asset space vehicle. National asset space vehicles generally support the national security of the United States. Class B space vehicles are low risk (most practical measures are taken to reduce risk), high importance to national security or safety (such as a high impact weather satellite), high confidence of success space vehicle (the highest procurement and assurance standards are used) with required moderate to long on-orbit life for a given orbit and represent the best industry standards for high reliability, high quality, and long design life space vehicle.

A Class B space vehicle may be an operational asset.

Class C

A demonstration space vehicle. Demonstration space vehicles generally utilize new technologies to demonstrate new space vehicle capabilities. Demonstration space vehicles are moderate risk, some application to national security, moderate confidence of success space vehicle with required short to moderate on-orbit life for a given orbit.

A Class C space vehicle is not an operational asset.

Class D

A proof of concept or fast turn-around space vehicle. Proof of concept and fast turnaround space vehicles generally are used to test new concepts or provide a high risk immediate capability in space. Class D space vehicles are high risk, little to no application to national security, low confidence of success space vehicles with required short on-orbit life for a given orbit.

Note: A Class D space vehicle is not an operational asset.

Appendix B. Example of a Robust FRACAS

For additional information of conducting Failure Review Boards and root cause analyses, reference:

- *Failure Review Board Guidance Document*, Aerospace Report No. TOR-2011(8591)-19
- *Root Cause Investigation (RCI) Best Practices Guide*, Aerospace Report No. TOR-2014-02202

A FRACAS should have the ability to sort by the following key fields:

- system
- subsystem
- part
- failure mode.

The table below outlines seven key steps that should be included in the failure report:

*** STEP 1: IDENTIFY THE PROBLEM STATEMENT**	
Who reported the problem?	
What is the defect?	
When was the issue discovered? Is it continuous, patterned, or sporadic? When is issue experienced?	
Where is the defect observed?	
What is the likelihood of recurrence with no further action taken? Is the occurrence singular or multiple?	
What requirement(s) were violated? • Customer terms (contract, drawing, etc.)	
How large is the issue? • How many objects have the problem? • How severe is the problem?	
Final Problem Statement (utilizing all information collected above)	
STEP 2: ESTABLISH THE TEAM **List team members/function assigned to work this issue:**	
Name	**Function**

STEP 3: DEVELOP INTERIM CONTAINMENT ACTION PLAN **Emergency Response – (Protect the customer from the problem)**				
Quantity Date Contained Who Notified Date Notified Serial Numbers Contract Number Shipment Tracking #				
Short Term Corrective Action Plan Development				
What was done for immediate action?	**Action Item**	**Assigned to**	**Target Due Date**	**Completion Date**
Short Term Corrective Action Plan Statement (utilizing all information collected above)				

*** STEP 4: COMPLETE THE ROOT CAUSE ANALYSIS** Click on link to access:	
Fault Tree Analysis conducted and attached:	Yes No
Cause and Effect Analysis conducted and attached:	Yes No
Brainstorming conducted and attached:	Yes No
5 Why Analysis conducted and attached:	Yes No
Process Flow Diagram conducted and attached	Yes No
FMEA conducted and attached:	Yes No
Other Tool conducted and attached: _____	Yes No
	(**BOLD** or Circle selection)

Potential Root Cause Determinations and/or Process Escape Points (Please Prioritize)	**Has Root Cause been Tested?**	**Can the problem be turned on and off by this Root Cause?**
Root Cause Analysis Statement (utilizing all information collected above)		

*** STEP 5: DEVELOP PERMANENT CORRECTIVE ACTION PLAN**				
Permanent Corrective Action Plan Development				
The Corrective Action Plan MUST address every Root Cause identified, and must contain at least one action for each cause.	**Action Item** Provide detailed plan for implementation	**Assigned to**	**Target Due Date**	**Completion Date**
1.				
Permanent Corrective Action Plan Statement (utilizing all information collected above)				

*** STEP 6: COMPLETE VERIFICATION OF PERMANENT CORRECTIVE ACTIONS**			
Was the corrective action plan implemented? Were all escape points addressed? Identify the steps taken to complete verification.	**Verification Steps**	**Assignee**	**Date**
	1.		
	2.		
	3.		
	4.		
Verification (utilizing all information collected above)			
*** STEP 7: VALIDATE PERMANENT CORRECTIVE ACTIONS**			
Was the change sustainable with no documentation of repeat issue? Did the corrective action plan permanently correct the root cause? Identify the steps taken to complete validation.	Validation Steps	Assignee	Date
	1.		
	2.		
	3.		
	4.		
	5.		
	6.		

AEROSPACE REPORT NO.
TOR-2015-02545

Design Review Improvement Recommendations

Approved Electronically by:

Todd M. Nygren, GENERAL MANAGER
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

Jacqueline M. Wyrwitzke, PRINC DIRECTOR
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

Philip B. Grant, PRINC DIRECTOR
ELECTRONICS ENGINEERING SUBDIVISION
ELECTRONICS & SENSORS DIVISION
ENGINEERING & TECHNOLOGY GROUP

Jackie M. Webb-Larkin, SECURITY SPECIALIST III
GOVERNMENT SECURITY SECURITY OPERATIONS
OPERATIONS & SUPPORT GROUP

Technical Peer Review Performed by:

Jacqueline M. Wyrwitzke, PRINC DIRECTOR
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

Cheryl L. Sakaizawa, ADMINISTRATIVE SPEC III
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

Richard K. Covington, DIRECTOR DEPT
DIGITAL & INTEGRATED CIRCUIT ELECT DEPT
ELECTRONICS ENGINEERING SUBDIVISION
ENGINEERING & TECHNOLOGY GROUP

SK0794